

DIRECTOR OF CENTRAL INTELLIGENCE
SECURITY COMMITTEE
COMPUTER SECURITY SUBCOMMITTEE

28 October 1981
DCISEC-CSS-M140

STAT - 1. The One Hundred and Fortieth meeting of the Computer Security Subcommittee was held on 20 October 1981 at [REDACTED], McLean, VA. The meeting was convened at 0930, and in attendance were:

STAT [REDACTED] Chairman

STAT [REDACTED] Executive Secretary

STAT [REDACTED] CIA

[REDACTED] CIA

Mr. Robert Graytock, Department of Justice

Mr. Carl Martz, Navy

STAT Mr. Lynn McNulty, Department of State

[REDACTED] NSA

Mr. Robert Storck, FBI

Mr. James Studer, Army

STAT Mr. James Schenken, U.S. Secret Service

[REDACTED] SECOM

2. The minutes from the previous meeting were reviewed; there were no changes or comments (although it was pointed out that one of the enclosures had been included twice), and thus the minutes were accepted as written.

STAT 3. [REDACTED] started the meeting with a review of pertinent discussions from the annual SECOM seminar, held at [REDACTED]. Among the topics which came up for discussion were the revised DCID, and the situation at the International Institute for Applied Systems Analysis (IIASA) in Vienna, Austria. [REDACTED] stated that there was a general expression of concern over the computer security problem, and that there was a desire expressed for tutorial material (e.g., films, videotapes) available for distribution within the Intelligence Community, which could be used as part of a general security education program. It was pointed out that, for anyone interested in a more complete review of the proceedings, minutes of the seminar will be distributed to the SECOM members.

STAT 4. The issue of administrative support to the Subcommittee was reviewed; [REDACTED] pointed out that the SECOM itself is very short of secretarial/admin support, and thus he felt it was not very likely that the Subcommittee could expect to obtain full-time support. However, it was suggested that the SECOM or the IC Staff might consider augmenting their present staff with someone whose duties would include (if not be dedicated to) supporting all the SECOM committees. [REDACTED] stated that he would bring this subject up to the SECOM as a recommendation of the CSS.

5. There was a rather lengthy discussion of the problem of industrial security, particularly that of assuring that security procedures for the handling of classified material are being followed. Although the problem was acknowledged by all, some of the members questioned whether the Subcommittee should be addressing this issue, stating the opinion that it was more a problem for the contracting officer than a computer security concern.

6. The Subcommittee next discussed the subject of the revision to DCID 1/16. The NSA member distributed copies of a proposed statement (a copy of which is enclosed) of the DCID, and presented an informal briefing of the approach taken and the justification for it. Basically, the proposed approach is to offer a simple (essentially obvious) policy statement, to the effect that the approval authority is responsible for providing protection of SCI in accordance with published policy/guidelines for the specific SCI being handled by the system. The paper then delineates the authority being bestowed, and the responsibilities which fall upon the approving authority. In the NSA approach, the definition of modes could remain in a technical guidance portion, but would serve only as examples of allowable operational environments, rather than delimiting the only allowable cases, as in the present version of the DCID. It was felt that such an approach, coupled with sufficient technical guidance/support would allow the approval authority to structure an operational environment which took into account all the myriad factors which affect total system security (e.g., user mix, clearances, sensitivity of data, user capabilities, technical capabilities of the ADP equipment, special hardware/software security features, etc.). Thus, the decision as to whether to allow a multilevel environment or to impose severe restrictions could be made by the approval authority strictly on the basis of the system operational requirements, security requirements, and the strength of the system's security features/mechanisms. The discussion which followed was largely based upon the relative merits of a "loose" approach versus the present "hard" definition of allowable modes. Mr. McNulty expressed a desire for including some accountability mechanisms and procedures which would be aimed at assuring uniform application of the policy.

7. There was a request for a copy of the Director, NSA's speech to the IEEE concerning the newly formed DoD Computer Security Center at NSA. A copy of this speech is enclosed.

8. The next meeting was set for 0930 on 17 November at [redacted]. The chairman asked that CIA, Army, and Department of State be prepared to present their views on the basic policy statement for the DCID.

[redacted]
Executive Secretary

Encls:
a/s

ADDRESS BY LTG LINCOLN D. FAURER, DIRECTOR NSA
AT IEEE COMPUTER CONFERENCE 81, WASHINGTON, D.C.

15 SEPTEMBER 1981

I WANT TO START OFF BY EXPRESSING MY THANKS TO DR. MILLS AND IEEE OFFICIALS FOR THE OPPORTUNITY TO COME HERE THIS MORNING AND TELL YOU ABOUT THE NEW DEPARTMENT OF DEFENSE COMPUTER SECURITY CENTER. I SAY "NEW" BECAUSE THE ASSIGNMENT OF THIS JOB TO MY AGENCY IS VERY RECENT. BUT IN POINT-OF-FACT, WE HAVE BEEN INVOLVED IN WORK IN THIS AREA FOR A NUMBER OF YEARS, IN SUPPORT OF OUR INTERNAL COMPUTER PROCESSING ACTIVITIES AND IN SUPPORT OF DEFENSE COMMUNICATIONS SYSTEMS ACQUISITION EFFORTS, SUCH AS THE PACKET-SWITCHED NETWORK, AUTODIN II.

FIRST, A BIT OF BACKGROUND. AS MANY OF YOU IN THIS CONFERENCE KNOW, CONCERN HAS GROWN IN RECENT YEARS ABOUT THE PROBLEM OF MAINTAINING THE SECURITY OF INFORMATION IN AN INCREASINGLY AUTOMATED COMMERCIAL AND FEDERAL WORLD. LAST YEAR, MY PREDECESSOR, ADMIRAL INMAN, NOW DEPUTY DIRECTOR OF THE CIA, WORKING WITH THE OFFICE OF THE SECRETARY OF DEFENSE EXAMINED THE NEED FOR A TECHNICAL CENTER TO SUPPORT THE MILITARY AND DEFENSE AGENCIES. THIS LED TO A LETTER ON THE FIRST OF JANUARY THIS YEAR FROM THE DEPUTY SECRETARY OF DEFENSE WHICH DIRECTED NSA TO ESTABLISH A CENTER FOR COMPUTER SECURITY EVALUATION. SINCE THEN WE HAVE BEEN BUSY CONSOLIDATING THE INTERNAL COMPUTER SECURITY ACTIVITIES OF NSA AND DEVELOPING THE RESOURCE REQUIREMENTS TO SUPPORT THE CENTER. THIS ORGANIZATION WAS FORMALLY ESTABLISHED WITHIN MY AGENCY IN JULY.

THIS MORNING, I WOULD LIKE TO TALK WITH YOU ABOUT THE NEEDS FOR IMPROVEMENTS IN COMPUTER SECURITY AND ALSO THE OTHER CHALLENGES WE WILL FACE. BUT MOST IMPORTANTLY--WHAT IT IS THIS CENTER WILL, AND WILL NOT DO. I SHOULD ALSO LIKE TO TAKE THIS OPPORTUNITY TO CLEAR UP ANY MISUNDERSTANDINGS ABOUT THE WAY WE WILL CONDUCT COMPUTER SECURITY ACTIVITIES AT NSA. I HAVE HEARD SOME ANXIETIES EXPRESSED BY INDUSTRY AND BY OTHERS AND I WOULD LIKE TO CLARIFY OUR INTENTIONS AS MUCH AS POSSIBLE.

AS I HAVE INTIMATED, THE CONCERN WITHIN DEFENSE ABOUT COMPUTER SECURITY IS A VERY GENUINE ONE. WE LIVE IN A FAST-PACED AND TECHNOLOGY INTENSIVE WORLD. FOR THE MILITARY SERVICES AND THE OTHER DEFENSE AGENCIES, THE PROBLEM WE FACE IS AN EXPLOSION OF INFORMATION, CLASSIFIED AT VARIOUS LEVELS OF DIFFERING SENSITIVITIES. OUR WORLD IS FILLED WITH AUTOMATIC DATA PROCESSING EQUIPMENT, GEOGRAPHICALLY DISPERSED AND OFTEN NETWORKED

TOGETHER. THE THREAT TO SECURITY RANGES FROM THE INADVERTENT DUMP OF MATERIAL TO A NONAUTHORIZED RECIPIENT ALL THE WAY TO DELIBERATE PENETRATION.

I DON'T MEAN TO IMPLY THAT INDIVIDUAL DEFENSE AGENCIES AND SERVICES HAVEN'T RECOGNIZED OR TRIED TO TACKLE THE PROBLEM. FOR EXAMPLE, WE HAVE TRIED TO DEAL WITH THE PROBLEM BY USING TIGER TEAMS TO DELIBERATELY PENETRATE OUR SYSTEMS. THEY ALMOST ALWAYS SUCCEED IN ATTAINING ACCESS, SOMETIMES USING SUCH SOPHISTICATED EFFORTS THAT THEY LEAVE NO TRACE OF THE ATTEMPT TO PENETRATE THE SYSTEM. SUCH EFFORTS WERE USUALLY FOLLOWED BY TECHNICAL EFFORTS TO CORRECT WEAKNESSES. UNFORTUNATELY THIS TYPE OF CORRECTIVE EFFORT WAS GENERALLY UNSUCCESSFUL AND UNREWARDING. FURTHERMORE, THE CORRECTIVE EFFORTS OFTEN SERIOUSLY DEGRADED PERFORMANCE. THE AIR FORCE TOOK THE LEAD ON A MORE SUCCESSFUL PROGRAM INVOLVING SECURITY KERNEL TECHNOLOGY. THE MOST SUCCESSFUL EFFORT WAS THE SECURITY-ENHANCED MULTICS SYSTEM THAT HAS BEEN RUNNING FOR SEVERAL YEARS IN THE PENTAGON.

A SIGNIFICANT AMOUNT OF TECHNOLOGY IS NOW AVAILABLE, BUT IT IS DIFFICULT FOR INDIVIDUAL USERS TO UNDERSTAND WHAT IT IS AND IS NOT CAPABLE OF ACHIEVING. A TECHNICAL ORGANIZATION TO RESPOND TO THE PROBLEMS OF THE INDIVIDUAL DOD AGENCIES SEEMS CALLED FOR.

- THERE ARE CLEAR REQUIREMENTS FOR SUPPORT TO SUCH ORGANIZATIONS IN THE NATIONAL SECURITY ESTABLISHMENT FOR EVALUATION OF NEW TECHNOLOGY.

- THERE ARE REQUIREMENTS FOR SYSTEMATIC CERTIFICATION AND ACCREDITATION OF SYSTEMS TO BE OPERATED IN A VARIETY OF ENVIRONMENTS.

- THERE IS A NEED FOR BASIC RESEARCH AND DEVELOPMENT TO BE CONSIDERABLY ACCELERATED.

ONE MIGHT ASK--WHY CHOOSE NSA FOR THE CENTER. I THINK THERE ARE SOME STRAIGHTFORWARD ANSWERS.

- WE ARE A LARGE AND VERY TECHNICAL ORGANIZATION.

- WE HAVE A LARGE WORK FORCE OF SCIENTIFIC AND OTHER PROFESSIONAL TALENTS THAT PROVIDE THE CRITICAL MASS FROM WHICH TO DRAW THE CORE OF MANPOWER NECESSARY TO FORM THE CENTER. WE CAN TAKE CONSIDERABLE ADVANTAGE OF OUR WORK IN RELATED AREAS.

- ALTHOUGH COMPUTER SECURITY SUPPORT IS A DISTINCT AND INDEPENDENT FUNCTION, THE NEED TO EXPLOIT ADVANCED TECHNOLOGY CLOSELY PARALLELS THE RESPONSIBILITY OF NSA TO OUR NATIONAL GOVERNMENT FOR THE SECURITY OF ITS COMMUNICATIONS.

AN INITIATIVE IN COMPUTER SECURITY IS NOT WITHOUT ITS PROBLEMS AND ITS CHALLENGES. THE MAJORITY OF COMPUTER SYSTEMS IN USE SIMPLY DO NOT HAVE SECURITY OF DATA AS THEIR PRIMARY OBJECTIVE. USERS ARE MOST INTERESTED IN PERFORMANCE, RELIABILITY, EASE OF USE, AND ACCESSIBILITY--AS THEY SHOULD BE. CONTEMPORARY COMPUTER SYSTEMS SIMPLY DO NOT PROVIDE RELIABLE PROTECTION OF THEIR DATA, AND CONTEMPORARY SYSTEMS ARE OFTEN DISTRIBUTED, WITH SECURITY PROBLEMS COMPOUNDED BY REMOTED TERMINAL OR NETWORK CONSIDERATIONS. DESPITE THE PROGRESS THAT HAS BEEN MADE, THERE IS A MAJOR SHORTAGE OF GOOD COMPUTER SECURITY TECHNOLOGY. INDUSTRY LEADERS HAVE TOLD US THAT THIS SITUATION WILL CONTINUE, IN THE ABSENCE OF A CERTAIN COMMERCIAL MARKET WILLING TO PAY FOR SUCH PRODUCTS. WE ALSO OBSERVE THAT SUCH TECHNOLOGY AS DOES EXIST DOES NOT ENJOY WIDESPREAD USE. THERE ARE MANY REASONS FOR THIS; IGNORANCE OF THE ATTRIBUTES OF THE PRODUCT, PERFORMANCE DEGRADATION THAT IS UNACCEPTABLE, OR COST.

MANAGEMENT AWARENESS OF THE PROBLEM ACROSS THE DEPARTMENT OF DEFENSE NEEDS CONSIDERABLE BOLSTERING. THIS IS NOT AN EASY MATTER! COMPUTER SECURITY ASPECTS OF COMPUTER OPERATIONS ARE VIEWED BY MOST AS A BLACK ART, AND MOST OFFICIALS CAN HARDLY BE BLAMED FOR SIMPLY SETTLING FOR ASSURANCES THAT THEY ARE IN COMPLIANCE WITH COMPUTER SECURITY REGULATIONS. I MUST CONFESS THAT AN INFORMED VIEW IS THAT THE CREATION OF POLICY AND REGULATION ON THIS ISSUE HAVE, IN A SENSE, BEEN GEARED TO THE TECHNOLOGY AVAILABLE TO SUPPORT IT. AS ONE OF OUR SENIOR PROFESSIONALS OBSERVED IN AN ARTICLE SEVERAL YEARS AGO, "A COMPUTER MAY WELL SATISFY ALL REGULATIONS AND STILL BE HIGHLY VULNERABLE."

BUT AS I HAVE ALLUDED TO EARLIER, PERHAPS THE BIGGEST CHALLENGE WE FACE IS THE ENORMOUS RELIANCE WE MUST PLACE ON INDUSTRY. COMPUTER SECURITY FEATURES ARE NECESSARILY PRODUCT-PECULIAR AND WE MUST FIND WAYS TO WORK CLOSELY WITH INDUSTRY TO HELP PRODUCE TRUSTED COMPUTER SYSTEMS. CLEARLY, IF I AM CORRECT IN MY ASSERTION THAT THERE IS A DISTINCT SHORTAGE OF RELIABLE SECURITY FEATURES, AND THAT THE BULK OF THE PRODUCTS WILL HAVE TO BE COMMERCIALY PRODUCED, THEN WE WILL OWE IT TO OUR DOD CUSTOMERS TO KEEP THE PRESSURE ON INDUSTRY TO PRODUCE. THAT PRESSURE WILL NEED TO BE SUSTAINED UNTIL MARKET AWARENESS IS GENERATED AND SECURITY OF INFORMATION, AND OF COMPUTER PROCESSES THEMSELVES, BECOME A MAJOR DESIGN GOAL FOR NEW COMMERCIAL SYSTEMS UNDER DEVELOPMENT BY THE MAJOR VENDORS.

NOW I WOULD LIKE TO TELL YOU ABOUT THE SPECIFIC THINGS THE COMPUTER SECURITY CENTER WILL DO. THESE FALL INTO FOUR AREAS: RESEARCH AND DEVELOPMENT, ASSISTANCE IN THE ACQUISITION OF DOD COMPUTER SYSTEMS, DISSEMINATION OF COMPUTER SECURITY INFORMATION, AND EVALUATION OF COMMERCIAL COMPUTER SECURITY PRODUCTS.

FIRST LET ME ADDRESS OUR CONDUCT AND SUPPORT OF RESEARCH AND DEVELOPMENT (R&D). AS I NOTED BEFORE, THE ABSENCE OF

TECHNOLOGY IS A MAJOR PROBLEM. I BELIEVE WE NEED AN ACTIVE, WELL-FORMED R&D PROGRAM. THIS WORK MUST, OF COURSE, BE TECHNICALLY SOUND; BUT, IN ADDITION, IT MUST BE CLEARLY FOCUSED ON TECHNOLOGY GAPS WHERE, IF SUCCESSFUL, THE RESEARCH WILL HAVE A SIGNIFICANT PAY-OFF IN TERMS OF DOD COMPUTER SECURITY. BOTH THE IN-HOUSE WORK AND THE SPONSORED RESEARCH IN INDUSTRY AND UNIVERSITIES WILL BE PART OF A COHESIVE PROGRAM WITH SEVERAL FACETS.

- WE WILL EXPLORE THE IMPLICATIONS OF SECURITY ON HARDWARE AND SOFTWARE ARCHITECTURES FOR VARIOUS COMPUTER COMPONENTS SUCH AS DATA BASE SYSTEMS AND MICROPROCESSORS.

- WE WILL LOOK FOR MORE EFFECTIVE WAYS TO PROVIDE SECURITY IN NETWORKS, ADDRESSING ISSUES SUCH AS COMMUNICATIONS PROTOCOLS AND END-TO-END ENCRYPTION.

- WE WILL SPECIFICALLY WORK ON VERIFICATION TOOLS TO ASSIST US IN EVALUATING WHETHER THE SECURITY FEATURES OF COMPUTER AND NETWORK SYSTEMS ARE TRULY EFFECTIVE.

- A SIGNIFICANT THRUST WILL BE DIRECTED TOWARDS APPLYING THE EMERGING RESEARCH RESULTS TO REPRESENTATIVE PROBLEMS WHERE THE CRITICAL ISSUES OF PERFORMANCE AND FUNCTIONALITY CAN BE ASSESSED.

THESE DEVELOPMENTS WILL BE SELECTED TO PROVOKE THE ASSIMILATION OF THE TECHNOLOGY INTO INDUSTRY PRODUCTS. THE RECENTLY ANNOUNCED HONEYWELL SECURE COMMUNICATION PROCESSOR IN THEIR LEVEL 6 MINICOMPUTER PRODUCT LINE SERVES AS AN EXAMPLE OF THIS PROCESS: THIS PRODUCT WAS BASED DIRECTLY ON PREVIOUS DOD SPONSORED RESEARCH THAT PRODUCED THE SECURITY KERNEL TECHNOLOGY.

AND I WOULD POINT OUT ANOTHER IMPORTANT CHARACTERISTIC OF OUR R&D: WE ARE COMMITTED TO HAVING THE RESEARCH DONE AND THE RESULTS DISSEMINATED IN AN OPEN AND UNCLASSIFIED MANNER, EXCEPT IN THOSE EXCEPTIONAL CASES WHERE WE ARE WORKING ON A PREVIOUSLY CLASSIFIED BASE. OUR MOTIVATION SHOULD BE CLEAR--THE TRANSFER OF THE TECHNOLOGY INTO COMPUTER SECURITY PRODUCTS THAT DOD CAN, IN TURN, PURCHASE IS GREATLY RESTRICTED IF THE RESEARCH RESULTS ARE CLASSIFIED OR OTHERWISE RESTRICTED. IN SHORT, I EXPECT OUR R&D TO BE OPENLY AVAILABLE, SIGNIFICANT IN ITS RESULTS, COMPLEMENTARY TO THE WORK OF OTHERS, AND RELEVANT TO DOD AND THE OTHER ORGANIZATIONS OF THE NATIONAL SECURITY ESTABLISHMENT.

OUR SECOND MAJOR TASK IN THE CENTER IS ASSISTING THE DOD ELEMENTS IN THE ACQUISITION AND TESTING OF TRUSTED SYSTEMS. THE BEST TECHNOLOGY IN THE WORLD IS OF LITTLE VALUE UNTIL WE HAVE PUT IT INTO OPERATION.

- AS A STARTING POINT, THE SPECIFICATIONS FOR THE ACQUISITION OF A NEW SYSTEM MUST CLEARLY STATE WHAT COMPUTER SECURITY CAPABILITIES ARE REQUIRED. IN THE PAST, REQUIREMENTS HAVE NOT ALWAYS BEEN CLEARLY AND CONSISTENTLY SPECIFIED. TO HELP REDRESS THIS PROBLEM, THE CENTER WILL DEVELOP A SET OF SECURITY STANDARDS AND CORRESPONDING INPUTS FOR USE IN PROCUREMENT SPECIFICATIONS. THESE WILL EVOLVE AND GROW AS THE TECHNOLOGY ADVANCES SO THAT DOD CAN TAKE FULL ADVANTAGE OF THE ALTERNATIVES AVAILABLE. FRANKLY, OUR INTENTION IS TO SIGNIFICANTLY REWARD THOSE DOD SUPPLIERS WHO PRODUCE THE COMPUTER SECURITY PRODUCTS THAT WE NEED.

- BEFORE A DOD ELEMENT CAN OPERATE A TRUSTED SYSTEM, REGULATIONS REQUIRE A CERTIFICATION AND ACCREDITATION PROCESS. THIS PROCESS PROVIDES THE BASIS FOR A JUDGMENT BY THE APPROPRIATE APPROVING AUTHORITY THAT THE SYSTEM SHOULD ACTUALLY BE TRUSTED FOR THE SIMULTANEOUS PROCESSING OF MULTIPLE LEVELS OF CLASSIFIED OR SENSITIVE INFORMATION. AGAIN, THE CENTER WILL PROVIDE AN EVOLVING SET OF TECHNICAL STANDARDS AND CRITERIA TO AID IN MAKING THESE JUDGMENTS.

- FOR SELECTED SYSTEMS OF PARTICULAR IMPORTANCE TO DOD, THE CENTER WILL DIRECTLY PARTICIPATE IN THIS ACQUISITION PROCESS. THIS WILL BE IN THE FORM OF TECHNICAL SUPPORT, TAILORED TO THE UNIQUE PROBLEMS OF A PARTICULAR SYSTEM.

IT SHOULD BE CLEAR THAT I EXPECT THE CENTER TO HAVE MAJOR, POSITIVE INFLUENCE ON THE SECURITY OF THE COMPUTER SYSTEMS THAT ARE BROUGHT INTO THE DOD INVENTORY. SHOULD SOME SUPPLIER CHOOSE NOT TO KEEP UP, THEY CAN EXPECT TO BE LEFT BEHIND. TO ACHIEVE THIS IMPACT, A LOT OF INFORMATION MUST BE EXCHANGED. THUS, A THIRD CENTER FUNCTION IS PROVIDING COMPUTER SECURITY DATA CENTER SERVICES.

- WE WILL PROVIDE A CONSOLIDATED SET OF INFORMATION ON THE VARIOUS COMPUTER SECURITY PRODUCTS THAT EXIST IN THE COMMERCIAL AND GOVERNMENT SECTORS, AS A SERVICE TO OUR CUSTOMERS.

- WE WILL ACTIVELY PARTICIPATE IN FOSTERING AN INCREASING AWARENESS OF COMPUTER SECURITY PROBLEMS AND SOLUTIONS. FOR DOD PERSONNEL WE WILL ASSIST IN IDENTIFYING WORTHWHILE OPPORTUNITIES FOR COMPUTER SECURITY EDUCATION, TRAINING, SEMINARS, AND WORKSHOPS: WE WILL ORGANIZE AND CONDUCT SUCH ACTIVITIES OURSELVES WHERE NEEDED. FURTHERMORE, WE EXPECT TO BE ACTIVE IN PUBLIC FORUMS--SUCH AS THIS IEEE CONFERENCE--TO KEEP YOU IN THE COMPUTER INDUSTRY INFORMED ON OUR ACTIVITIES AND, OF COURSE, TO LEARN ABOUT WHAT YOU ARE DOING.

- WE WILL OBVIOUSLY PROVIDE A REPOSITORY FOR THE VARIOUS STANDARDS AND CRITERIA DEVELOPED BY THE CENTER FOR USE WITHIN DOD.

THE EFFECTIVE EXCHANGE OF INFORMATION ON COMPUTER SECURITY IS TOO IMPORTANT TO BE LEFT TO CHANCE. THEREFORE, THE CENTER WILL MAKE IT ITS BUSINESS TO STIMULATE AND FACILITATE THIS EXCHANGE.

THE FINAL FUNCTION I WANT TO TALK ABOUT IS THE EVALUATION OF COMMERCIAL COMPUTER SECURITY PRODUCTS. LET ME FIRST DISTINGUISH THIS FROM THE CENTER'S ASSISTANCE TO COMPUTER SYSTEMS ACQUISITION. THE ACQUISITION SUPPORT THAT I DESCRIBED EARLIER IS BASED ON THE UNIQUE ENVIRONMENT OF EACH DOD APPLICATION, AND ULTIMATELY SECURITY IS ADDRESSED ON A TOTAL SYSTEM BASIS THAT INCLUDES A WIDE RANGE OF FACTORS SUCH AS PHYSICAL, PERSONNEL, PROCEDURAL, TEMPEST AND COMMUNICATIONS SECURITY.

HOWEVER, WE FREQUENTLY FIND THAT A GIVEN VENDOR'S HARDWARE/SOFTWARE PRODUCT WILL SHOW UP IN A NUMBER OF DIVERSE DOD APPLICATIONS. THEREFORE, IT IS EXTREMELY VALUABLE TO HAVE A CAREFUL EVALUATION OF THE TECHNICAL MERIT OF THE PRODUCT ITSELF. THIS IS PARTICULARLY USEFUL WHEN SELECTING THE WINNER IN A COMPETITIVE PROCUREMENT, SINCE IT MAY BE IMPRACTICAL TO DO THE NECESSARY DETAILED EVALUATION FOR EVERY OFFEROR FOR EACH PROCUREMENT. THUS, WE CONTEMPLATE THE EVALUATION OF COMMERCIAL PRODUCTS AGAINST AN OBJECTIVE SET OF CRITERIA, INDEPENDENT OF ANY SPECIFIC DOD APPLICATION.

THIS EVALUATION OBVIOUSLY CAN ONLY BE BASED ON THE INFORMATION THAT IS AVAILABLE TO THE CENTER. THEREFORE, I WOULD EMPHASIZE THAT IN MOST CASES FOR A PRODUCT TO HAVE A POSITIVE EVALUATION RESULT, WE WILL NEED TO WORK COOPERATIVELY WITH THE MANUFACTURER. AS A MATTER OF FACT, THE OFFICE OF THE SECRETARY OF DEFENSE HAS ALREADY INITIATED A NUMBER OF SUCH COOPERATIVE EVALUATION EFFORTS, AND WE EXPECT TO CONTINUE AND EXPAND THESE EFFORTS UNDER THE AUSPICES OF THE CENTER.

- THE RESULT WILL BE AN EVALUATED PRODUCTS LIST FOR USE WITHIN THE NATIONAL SECURITY ESTABLISHMENT. THIS WILL BE BASED ON CRITERIA FOR DISTINCT LEVELS, OR "FIGURES OF MERIT."

- THIS EVALUATION WILL BE DONE ON AN OPEN BASIS. THE COOPERATING MANUFACTURER WILL BE PROVIDED THE RESULTS OF THE EVALUATION AND THE SUPPORTING RATIONALE. FURTHERMORE, THE FIGURE OF MERIT AND, AS APPROPRIATE, SUPPLEMENTAL COMMENTS WILL BE PUBLICLY AVAILABLE.

- HOWEVER, THE CENTER WILL RIGOROUSLY RESPECT THE CONFIDENTIALITY OF INFORMATION THAT IS SPECIFICALLY IDENTIFIED AS PROPRIETARY WHEN IT IS PROVIDED BY THE MANUFACTURER. FURTHERMORE, SPECIFIC VULNERABILITIES THAT ARE IDENTIFIED BY THE CENTER WITH THE MANUFACTURER'S COOPERATION WILL BE TREATED WITH SIMILAR CONFIDENTIALITY.

FINALLY, I WOULD LIKE TO CLEARLY DISTINGUISH BETWEEN MYTH AND REALITY IN REGARD TO THE ISSUE OF CLASSIFICATION FOR COMMERCIAL PRODUCTS. WE HAVE GIVEN CAREFUL THOUGHT TO THIS ISSUE, AND IF YOU WILL PERMIT ME TO CAREFULLY SET ASIDE FROM THIS DISCUSSION THE ISSUE OF PUBLIC CRYPTOGRAPHY AS IT APPLIES TO COMPUTER SECURITY, WE CANNOT CONCEIVE OF A CONDITION THAT WOULD REQUIRE CLASSIFICATION OF COMMERCIAL-DEVELOPED COMPUTER SOFTWARE OR HARDWARE SYSTEMS. FURTHERMORE, IT IS CLEAR THAT TO DO SO WOULD SEVERELY IMPAIR THE EFFECTIVENESS OF THE CENTER. AFTER ALL, WHAT MANUFACTURER WOULD COOPERATE IN THE EVALUATION OF HIS PRODUCT, IF THIS COULD POSSIBLY LEAD TO CLASSIFICATION THAT WOULD RESTRICT HIS SALE OF THAT PRODUCT?

NOW LEST I BE MISUNDERSTOOD, IT IS CONCEIVABLE THAT A PARTICULAR DOD COPY OF SUCH A PRODUCT MIGHT BE CONTROLLED AS CLASSIFIED TO PREVENT MALICIOUS TAMPERING WHILE BEING TRANSPORTED; SIMILARLY, SPECIFIC VULNERABILITIES IN THE CONTEXT OF A PARTICULAR DOD APPLICATION MIGHT BE CLASSIFIED. BUT THE IMPORTANT THING IS THAT NONE OF THESE SORT OF CLASSIFICATION ACTIONS WOULD IN ANY WAY RESTRICT THE DISTRIBUTION OF THIS PRODUCT IN THE PRIVATE SECTOR.

IN SUMMARY, LET ME SAY THAT WE HAVE A BIG JOB HERE. THIS IS A SERIOUS UNDERTAKING WHICH WILL TAKE SUBSTANTIAL RESOURCES, SMART PEOPLE AND LOTS OF HARD WORK. THE THREAT IS A REAL ONE; MADE MORE PRESSING BY THE VERY OPENNESS OF OUR SOCIETY AND RELATIVELY EASY TARGET WE REPRESENT. SECURITY CONTROLS MUST BE AS EFFECTIVE AS WE CAN HELP MAKE THEM WITHOUT SERIOUSLY INTERFERING WITH THE FUNDAMENTAL PURPOSE FOR WHICH THE SYSTEMS ARE ACQUIRED. TO MEET THESE OBJECTIVES, WE WILL AGGRESSIVELY PURSUE WELL-FOCUSED RESEARCH AND DEVELOPMENT TO PROVIDE IMPROVED TECHNOLOGY, AND WE WILL STIMULATE EFFECTIVE USE OF THE TECHNOLOGY WE ALREADY HAVE. TO FURTHER PROVOKE COMMERCIAL DEVELOPMENT, WE WILL INSIST THAT THE SYSTEMS WE BUY INCLUDE THOSE ACHIEVABLE SECURITY CAPABILITIES THAT WE NEED.

FINALLY, I WANT TO EMPHASIZE THAT THE SUCCESS OF THE COMPUTER SECURITY CENTER WILL REQUIRE THE CLOSEST INTERACTION WITH INDUSTRY, AND ALTHOUGH WE EMPHASIZE THE FREE AND OPEN EXCHANGE OF INFORMATION, WE WILL RESPECT THEIR PROPRIETARY RIGHTS. I MIGHT ADD THAT THIS CLOSE INTERACTION INCLUDES OTHER ELEMENTS OF THE TECHNOLOGY COMMUNITY--THE UNIVERSITIES, TECHNICAL INSTITUTES AND PROFESSIONAL ASSOCIATIONS SUCH AS YOU. AGAIN, MY THANKS TO YOU FOR THE OPPORTUNITY TO PRESENT MY VIEWS ON THIS SUBJECT AND FOR YOUR ATTENTION THIS MORNING.

file: ocid
as of: 10.10.81

DCID 1/16

PROTECTION OF FOREIGN INTELLIGENCE IN AUTOMATED DATA PROCESSING SYSTEMS AND NETWORKS

1. Purpose--This directive prescribes the authority and responsibilities of the National Foreign Intelligence Board (NFIb) members for the protection of foreign intelligence in automated data processing (ADP) systems and networks. This authority and responsibilities may be delegated as appropriate for the particular ADP system/network involved.

2. Applicability--This directive applies to all NFIb members and all other United States Government departments and agencies who process and/or store foreign intelligence in ADP systems and networks. It applies equally whether the ADP systems and networks are used, owned, and/or operated by the United States Government or by contractors or consultants for the United States Government.

3. Policy--The use of ADP systems and networks will in no way endanger foreign intelligence to compromise and exploitation. The required protection of foreign intelligence is defined in existing documentation (policy) which dictates the handling and access of specific compartments of foreign intelligence. The determination of whether an ADP system or network provides the required protection will be system/network specific. However, the basis for making this determination will be consistent and uniform throughout the NFIb community.

4. Authority--To insure uniformity in the protection of foreign intelligence a primary authority from among the NFIb members will be explicitly designated for each ADP system/network and all decisions made by the primary authority will be mutually agreed to by all the other NFIb users of each ADP system/network.

a. Single user system/network--The NFIb member who is the single user of an ADP system/network is designated the Approval Authority for that ADP system/network.

b. Shared system/network--One NFIb member will be designated as the Principal Approval Authority when an ADP system/network is jointly used by more than one NFIb member and all other NFIb members who share the use of that ADP system/network will be designated as Secondary Approval Authorities.

c. Concatenated systems/networks--When more than one system/network are interconnected or when a system is connected to a network of systems each NFIb member who is already designated as the Approval Authority or Principal Approval Authority of any of the systems/networks involved will become a member of the Joint Approval Authority for the concatenated systems/networks. The Principal Approval Authorities will represent any Secondary Approval Authorities of their respective systems/networks. One of the members of the Joint Approval Authority will be designated

Principal Joint Approval Authority but all members shall act as a common body for carrying out the responsibilities of the Joint Approval Authority.

5. Responsibility--

a. The Approval Authority, Principal Approval Authority and Joint Approval Authority will be responsible for:

1) Assuring the most economical and effective utilization of resources while complying with the policy stated above.

2) Identifying the information protection requirements for the specific ADP system/network based on applicable foreign intelligence protection policies.

3) Defining the set of protection measures/mechanisms that are required in the ADP system/network based on functionality of the system/network, user/operational environment, information characteristics, information protection policies, etc.

4) Performing the technical assessments, risk analyses, etc., upon which an accreditation/certification of the ADP system/network can be based.

5) Evaluating the ADP system/network for compliance with this policy and certifying such compliance.

6) Accrediting the ADP system/network and defining the allowable operational environments based on the assessments of security of the ADP system/network and a risk analysis.

7) Coordinating all of the above actions with the Secondary Approval Authorities to assure that all users of an ADP system/network mutually agree in the decisions made.

b. The Secondary Approval Authority will support the Principal Approval Authority in carrying out the responsibilities defined above and will participate equally with the Principal Approval Authority in the decisions made.

6. Supersession--This directive supersedes Director of Central Intelligence Directive No. 1/16, "Security of Compartmented Computer Operations", effective 16 May 1976. All other existing directives, regulations and other documents referencing the superseded directive shall be revised to reflect this supersession.

7. Implementation--Each of its member shall develop and promulgate implementing directives and regulations within one year from the effective date of this directive.

8. Review--This directive shall be reviewed within three years from its effective date.